5.2.5 Incident management

Key message

The purpose of the incident management practice is to minimize the negative impact of incidents by restoring normal service operation as quickly as possible.

Definition: Incident

An unplanned interruption to a service or reduction in the quality of a service.

Incident management can have an enormous impact on customer and user satisfaction, and on how customers and users perceive the service provider. Every incident should be logged and managed to ensure that it is resolved in a time that meets the expectations of the customer and user. Target resolution times are agreed, documented, and communicated to ensure that expectations are realistic. Incidents are prioritized based on an agreed classification to ensure that incidents with the highest business impact are resolved first.

Organizations should design their incident management practice to provide appropriate management and resource allocation to different types of incident. Incidents with a low impact must be managed efficiently to ensure that they do not consume too many resources. Incidents with a larger impact may require more resources and more complex management. There are usually separate processes for managing major incidents, and for managing information security incidents.

Information about incidents should be stored in incident records in a suitable tool. Ideally, this tool should also provide links to related CIs, changes, problems, known errors, and other knowledge to enable quick and efficient diagnosis and recovery. Modern IT service management tools can provide automated matching of incidents to other incidents, problems, or known errors, and can even provide intelligent analysis of incident data to generate recommendations for helping with future incidents.

It is important that people working on an incident provide good-quality updates in a timely fashion. These updates should include information about symptoms, business impact, CIs affected, actions completed, and actions planned. Each of these should have a timestamp and information about the people involved, so that the people involved or interested can be kept informed. There may also be a need for good collaboration tools so that people working on an incident can collaborate effectively.

Incidents may be diagnosed and resolved by people in many different groups, depending on the complexity of the issue or the incident type. All of these groups need to understand the incident management process, and how their contribution to this helps to manage the value, outcomes, costs, and risks of the services provided:

- Some incidents will be resolved by the users themselves, using self-help. Use of specific self-help records should be captured for use in measurement and improvement activities.
- Some incidents will be resolved by the service desk.
- More complex incidents will usually be escalated to a support team for resolution. Typically, the routing is based on the incident category, which should help to identify the correct team.
- Incidents can be escalated to suppliers or partners, who offer support for their products and services.
- The most complex incidents, and all major incidents, often require a temporary team to work together to identify the resolution. This team may include representatives of many stakeholders, including the service provider, suppliers, users, etc.
- In some extreme cases, disaster recovery plans may be invoked to resolve an incident. Disaster recovery is described in the service continuity management practice (section 5.2.12).

Effective incident management often requires a high level of collaboration within and between teams. These teams may include the service desk, technical support, application support, and vendors. Collaboration can facilitate information-sharing and learning, as well as helping to solve the incident more efficiently and effectively.

Tip

Some organizations use a technique called swarming to help manage incidents. This involves many different stakeholders working together initially,

until it becomes clear which of them is best placed to continue and which can move on to other tasks.

Third-party products and services that are used as components of a service require support agreements which align the obligations of the supplier with the commitments made by the service provider to customers. Incident management may require frequent interaction with these suppliers, and routine management of this aspect of supplier contracts is often part of the incident management practice. A supplier can also act as a service desk, logging and managing all incidents and escalating them to subject matter experts or other parties as required.

There should be a formal process for logging and managing incidents. This process does not usually include detailed procedures for how to diagnose, investigate, and resolve incidents, but can provide techniques for making investigation and diagnosis more efficient. There may be scripts for collecting information from users during initial contact, and this may lead directly to diagnosis and resolution of simple incidents. Investigation of more complicated incidents often requires knowledge and expertise, rather than procedural steps.

Dealing with incidents is possible in every value chain activity, though the most visible (due to effect on users) are incidents in an operational environment.

Figure 5.20 shows the contribution of incident management to the service value chain, with the practice being applied mainly to the engage, and deliver and support value chain activities. Except for plan, other activities may use information about incidents to help set priorities:

- Improve Incident records are a key input to improvement activities, and are prioritized both in terms of incident frequency and severity.
- Engage Incidents are visible to users, and significant incidents are also visible to customers. Good incident management requires regular communication to understand the issues, set expectations, provide status updates, and agree that the issue has been resolved so the incident can be closed.
- Design and transition Incidents may occur in test environments, as well as during service release and deployment. The practice ensures these incidents are resolved in a timely and controlled manner.
- Obtain/build Incidents may occur in development environments. Incident management practice ensures these incidents are resolved in a timely and controlled manner.
- Deliver and support Incident management makes a significant contribution to support. This value chain activity includes resolving incidents and problems.

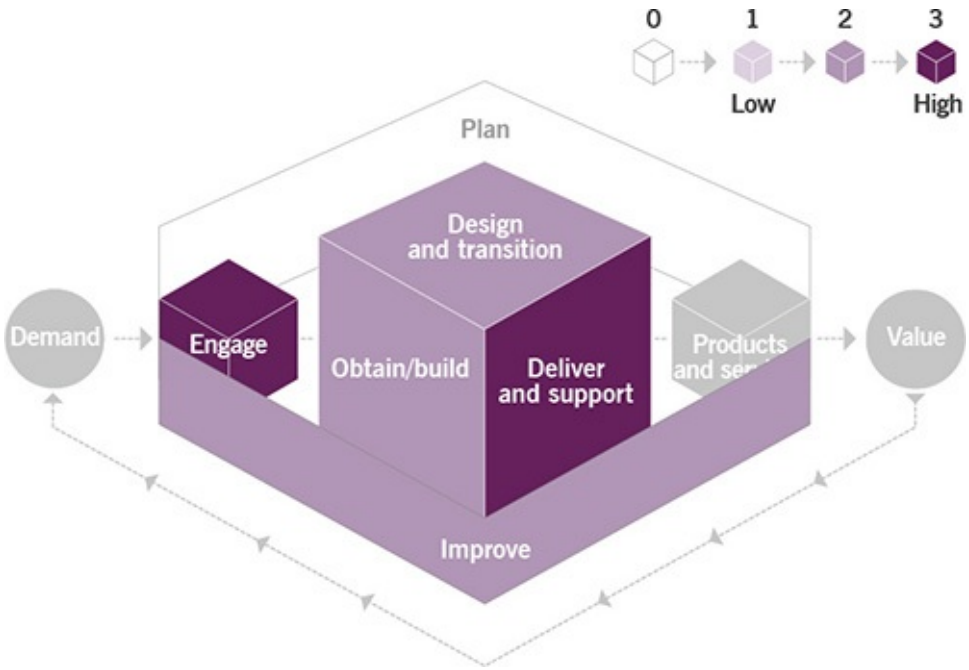

Figure 5.20 Heat map of the contribution of incident management to value chain activities

The ITIL story: Axle's incident management

Radhika: *Axle faces many potential IT and non-IT incidents. Cars can break down, road accidents might occur, or our customers might face challenges with unfamiliar road rules.*

Marco: *A car booking can be affected by an error in our app, or by a user getting lost due to a navigation error with our software. When incidents occur, we have to be ready to restore normal services as soon as possible. We also have to make sure our team knows how and when to switch from pre-defined recovery procedures to swarming and collective analysis.*

Radhika: *We also make sure that such cases are followed by investigation and improvements.*

Henri: *Axle has developed clear processes for all types of incidents, with workarounds available for cases that happen frequently, such as a tyre puncture or loss of internet connectivity.*

Radhika: *Our teams work together with our suppliers and partners to ensure fast and effective incident response. We develop and test recovery procedures together with the partners involved in any incidents we experience.*

5.2.6 IT asset management

Key message

The purpose of the IT asset management practice is to plan and manage the full lifecycle of all IT assets, to help the organization:

- maximize value
- control costs
- manage risks
- support decision-making about purchase, re-use, retirement, and disposal of assets
- meet regulatory and contractual requirements.

Definition: IT asset

Any financially valuable component that can contribute to the delivery of an IT product or service.

The scope of IT asset management typically includes all software, hardware, networking, cloud services, and client devices. In some cases, it may also include non-IT assets such as buildings or information where these have a financial value and are required to deliver an IT service. IT asset management can include operational technology (OT), including devices that are part of the Internet of Things. These are typically devices that were not traditionally thought of as IT assets, but that now include embedded computing capability and network connectivity.

Types of asset management

Asset management is a well-established practice that includes the acquisition, operation, care, and disposal of organizational assets, particularly critical

infrastructure.

IT asset management (ITAM) is a sub-practice of asset management that is specifically aimed at managing the lifecycles and total costs of IT equipment and infrastructure.

Software asset management (SAM) is an aspect of IT asset management that is specifically aimed at managing the acquisition, development, release, deployment, maintenance, and eventual retirement of software assets. SAM procedures provide effective management, control, and protection of software assets.

Understanding the cost and value of assets is essential to also comprehending the cost and value of products and services, and is therefore an important underpinning factor in everything the service provider does. IT asset management contributes to the visibility of assets and their value, which is a key element to successful service management as well as being useful to other practices.

IT asset management requires accurate inventory information, which it keeps in an asset register. This information can be gathered in an audit, but it is much better to capture it as part of the processes that change the status of assets, for example, when new hardware is delivered, or when a new instance of a cloud service is requested. If IT asset management has good interfaces with other practices, including service configuration management, incident management, change control, and deployment management, then the asset status information can be maintained with less effort. Audits are still needed, but these can be less frequent, and are easier to do when there is already an accurate asset register.

IT asset management helps to optimize the use of valuable resources. For example, the number of spare computers an organization requires can be calculated based on service level agreement commitments, the measured performance of service requests, and demand predictions from capacity and performance management.

Some organizations discover a need for IT asset management after a software vendor requests an audit of licence use. This can be very stressful if the required information has not been maintained, and can lead to significant costs, both in carrying out the audit and then paying any additional licence costs that are identified. It is much cheaper and easier to simply maintain information about software licence use as part of normal IT asset management activity, and to provide this in response to any vendor requests. Software runs on hardware, so the management of software and hardware assets should be combined to ensure that all licences are properly managed. For the same reason, the management of cloud-based assets should also be included.

The cost of cloud services can easily get out of control if the organization does not

manage these in the same way as other IT assets. Each individual use of a cloud service may be relatively cheap, but by spending in small amounts it is easy to consume much more resource than was planned, leaving the organization with a correspondingly large bill. Again, good IT asset management can help to control this.

The activities and requirements of IT asset management will vary for different types of asset:

- Hardware assets must be labelled for clear identification. It is important to know where they are and to help protect them from theft, damage, and data leakage. They may need special handling when they are re-used or decommissioned; for example, erasure or shredding of disk drives depends on information security requirements. Hardware assets may also be subject to regulatory requirements, such as the EU Waste Electrical and Electronic Equipment Directive.
- Software assets must be protected from unlawful copying, which could result in unlicensed use. The organization must ensure that licence terms are adhered to and that licences are only re-used in ways that are allowed under the contract. It is important to retain verified proof of purchase and entitlement to run the software. It is very easy to lose software licences when equipment is decommissioned, so it is important that the IT asset management process recovers these licences and makes them available for re-use where appropriate.
- Cloud-based assets must be assigned to specific products or groups so that costs can be managed. Funding must be managed so that the organization has the flexibility to invoke new instances of cloud use when needed, and to remove instances that are not needed, without the risk of uncontrolled costs. Contractual arrangements must be understood and adhered to, in the same way as for software licences.
- Client assets must be assigned to individuals who take responsibility for their care. Processes are needed to manage lost or stolen devices, and tools may be needed to erase sensitive data from them or otherwise ensure that this data is not lost or stolen with the device.

In all cases, the organization needs to ensure that the full lifecycle of each asset is managed. This includes managing asset provisioning; receiving, decommissioning, and return; hardware disposal; software re-use; leasing management; and potentially many other activities.

IT asset management maintains information about the assets, their costs, and related contracts. Therefore, the IT asset register is often combined (or federated) with the information stored in a configuration management system (CMS). If the two are separate then it is important that assets can be mapped between them, usually by use of a standard naming convention. It may also be necessary to combine (or federate) the IT asset register with systems used to manage other financial assets, or with systems used to manage suppliers.

In some organizations there is a centralized team responsible for IT asset management. This team may also be responsible for configuration management. In other organizations, each technical team may be responsible for management of the IT assets they support; for example, the storage team could manage storage assets while the networking team manages network assets. Each organization must consider its own context and culture to choose the appropriate level of centralization. However, having some central roles helps to ensure asset data quality and the development of expertise on specific aspects such as software licensing and inventory systems.

IT asset management typically includes the following activities:

- Define, populate, and maintain the asset register in terms of structure and content, and the storage facilities for assets and related media
- Control the asset lifecycle in collaboration with other practices (for example, upgrading obsolete software or onboarding new staff members with a laptop and mobile phone) and record all changes to assets (status, location, characteristics, assignment, etc.)
- Provide current and historical data, reports, and support to other practices about IT assets
- Audit assets, related media, and conformity (particularly with regulations, and licence terms and conditions) and drive corrective and preventive improvements to deal with detected issues.

Figure 5.21 shows the contribution of IT asset management to the service value chain, with the practice being applied mainly to the design and transition, and obtain/build value chain activities:

- Plan Most policies and guidance for IT asset management comes from the service financial management practice. Some asset management policies are driven by governance and some are driven by other practices, such as information security management. IT asset management can be considered a strategic practice that helps the organization to understand and manage cost and value.
- Improve This value chain activity must consider the impact on IT assets, and some improvements will directly involve IT asset management in helping to understand and manage costs.
- Engage There may be some demand for IT asset management from stakeholders. For example, a user may report a lost or stolen mobile phone, or a customer may require reports on the value of IT assets.
- Design and transition This value chain activity changes the status of IT assets, and so drives most IT asset management activity.
- Obtain/build IT asset management supports asset procurement to ensure that assets are traceable from the beginning of their lifecycle.

- Deliver and support IT asset management helps to locate IT assets, trace their movements, and control their status in the organization.

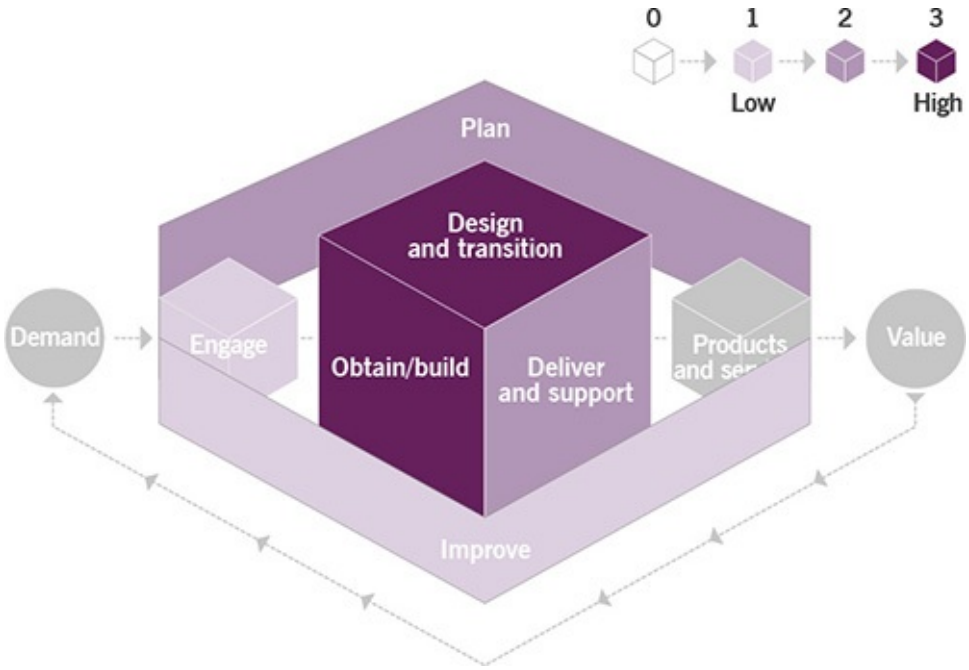

Figure 5.21 Heat map of the contribution of IT asset management to value chain activities

5.2.7 Monitoring and event management

Key message

The purpose of the monitoring and event management practice is to systematically observe services and service components, and record and report selected changes of state identified as events. This practice identifies and prioritizes infrastructure, services, business processes, and information security events, and establishes the appropriate response to those events, including responding to conditions that could lead to potential faults or incidents.

Definition: Event

Any change of state that has significance for the management of a service or other configuration item (CI). Events are typically recognized through notifications created by an IT service, CI, or monitoring tool.

The monitoring and event management practice manages events throughout their lifecycle to prevent, minimize, or eliminate their negative impact on the business.

The monitoring part of the practice focuses on the systematic observation of services and the CIs that underpin services to detect conditions of potential significance. Monitoring should be performed in a highly automated manner, and can be done actively or passively. The event management part focuses on recording and managing those monitored changes of state that are defined by the organization as an event, determining their significance, and identifying and initiating the correct control action to manage them. Frequently the correct control action will be to initiate another practice, but sometimes it will be to take no action other than to continue monitoring the situation. Monitoring is necessary for event management to take place, but not all monitoring results in the detection of an event.

Not all events have the same significance or require the same response. Events are often classified as informational, warning, and exceptions. Informational events do not require action at the time they are identified, but analysing the data gathered from them at a later date may uncover desirable, proactive steps that can be beneficial to the service. Warning events allow action to be taken before any negative impact is actually experienced by the business, whereas exception events indicate that a breach to an established norm has been identified (for example, to a service level agreement). Exception events require action, even though business impact may not yet have been experienced.

The processes and procedures needed in the monitoring and event management practice must address these key activities and more:

- identifying what services, systems, CIs, or other service components should be monitored, and establishing the monitoring strategy
- implementing and maintaining monitoring, leveraging both the native monitoring features of the elements being observed as well as the use of designed-for-purpose monitoring tools
- establishing and maintaining thresholds and other criteria for determining which

changes of state will be treated as events, and choosing criteria to define each type of event (informational, warning, or exception)

- establishing and maintaining policies for how each type of detected event should be handled to ensure proper management
- implementing processes and automations required to operationalize the defined thresholds, criteria, and policies.

This practice is highly interactive with other practices participating in the service value chain. For example, some events will indicate a current issue that qualifies as an incident. In this case, the correct control action will be to initiate activity in the incident management practice. Repeated events showing performance outside of desired levels may be evidence of a potential problem, which would initiate activity in the problem management practice. For some events, the correct response is to initiate a change, engaging the change control practice.

Although the work of this practice, once put in place, is highly automated, human intervention is still required, and is in fact essential. For the definition of monitoring strategies and specific thresholds and assessment criteria, it can help to bring in a broad range of perspectives, including infrastructure, applications, service owners, service level management, and representation from the warranty-related practices. Remember that the starting point for this practice is likely to be simple, setting the stage for a later increase in complexity, so it is important that the expectations of participants are managed.

Organizations and people are also critical to providing an appropriate response to monitored data and events, in alignment with policies and organizational priorities. Roles and responsibilities must be clearly defined, and each person or group must have easy, timely access to the information needed to perform their role.

Automation is key to successful monitoring and event management. Some service components come equipped with built-in monitoring and reporting capabilities that can be configured to meet the needs of the practice, but sometimes it is necessary to implement and configure purpose-built monitoring tools. The monitoring itself can be either active or passive. In active monitoring, tools will poll key CIs, looking at their status to generate alerts when an exception condition is identified. In passive monitoring, the CI itself generates the operational alerts.

Automated tools should also be used for the correlation of events. These features may be provided by monitoring tools or other tools such as ITSM workflow systems. There can be a huge volume of data generated by this practice, but without clear policies and strategies on how to limit, filter, and use this data, it will be of no value.

If third parties are providing products or services in the overall service architecture, they should also supply expertise in the monitoring and reporting capabilities of their offerings. Leveraging this expertise can save time when trying to operationalize monitoring and event management strategies and workflows. If some IT functions,

such as infrastructure management, are partially or wholly outsourced to a supplier, they may be reluctant to expose monitoring or event data related to the elements they manage. Don't ask for data that is not truly needed, but if data is required, make sure that the provision of that data is explicitly part of the contract for the supplier's services.

Figure 5.22 shows the contribution of monitoring and event management to the service value chain, with the practice being involved in all value chain activities except plan:

- Improve The monitoring and event management practice is essential to the close observation of the environment to evaluate and proactively improve its health and stability.
- Engage Monitoring and event management may be the source of internal engagement for action.
- Design and transition Monitoring data informs design decisions. Monitoring is an essential component of transition: it provides information about the transition success in all environments.
- Obtain/build Monitoring and event management supports development environments, ensuring their transparency and manageability.
- Deliver and support The practice guides how the organization manages internal support of identified events, initiating other practices as appropriate.

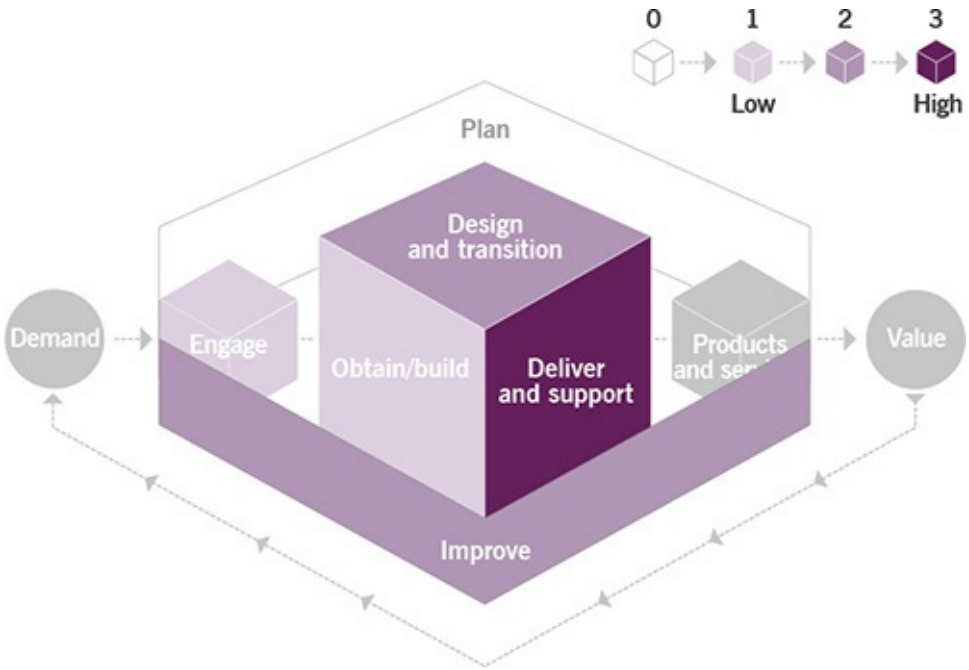

Figure 5.22 Heat map of the contribution of monitoring and event management to value chain activities

5.2.8 Problem management

Key message

The purpose of the problem management practice is to reduce the likelihood and impact of incidents by identifying actual and potential causes of incidents, and managing workarounds and known errors.

Definitions

- Problem A cause, or potential cause, of one or more incidents.
- Known error A problem that has been analysed but has not been resolved.

Figure 5.23 The phases of problem management

Every service has errors, flaws, or vulnerabilities that may cause incidents. They may include errors in any of the four dimensions of service management. Many errors are identified and resolved before a service goes live. However, some remain unidentified or unresolved, and may be a risk to live services. In ITIL, these errors are called problems and they are addressed by the problem management practice.

Problems are related to incidents, but should be distinguished as they are managed in different ways:

- Incidents have an impact on users or business processes, and must be resolved so that normal business activity can take place.
- Problems are the causes of incidents. They require investigation and analysis to identify the causes, develop workarounds, and recommend longer-term resolution. This reduces the number and impact of future incidents.

Problem management involves three distinct phases, as shown in Figure 5.23.

Problem identification activities identify and log problems. These include:

- performing trend analysis of incident records
- detection of duplicate and recurring issues by users, service desk, and technical support staff
- during major incident management, identifying a risk that an incident could recur
- analysing information received from suppliers and partners
- analysing information received from internal software developers, test teams, and project teams.

Other sources of information can also lead to problems being identified.

Problem control activities include problem analysis, and documenting workarounds and known errors.

Problems are prioritized for analysis based on the risk that they pose, and are managed as risks based on their potential impact and probability. It is not essential to analyse every problem; it is more valuable to make significant progress on the highest-priority problems than to investigate every minor problem that the organization is aware of.

Incidents typically have many interrelated causes, and the relationships between them can be complex. Problem control should consider all contributory causes, including causes that contributed to the duration and impact of incidents, as well as those that led to the incidents happening. It is important to analyse problems from the perspective of all four dimensions of service management. For example, an incident that was caused by inaccurate documentation may require not only a correction to that documentation but also training and awareness for support personnel, suppliers, and users.

When a problem cannot be resolved quickly, it is often useful to find and document a workaround for future incidents, based on an understanding of the problem. Workarounds are documented in problem records. This can be done at any stage; it doesn't need to wait for analysis to be complete. If a workaround has been documented early in problem control, then this should be reviewed and improved after problem analysis has been completed.

Definition: Workaround

A solution that reduces or eliminates the impact of an incident or problem for which a full resolution is not yet available. Some workarounds reduce the

likelihood of incidents.

An effective incident workaround can become a permanent way of dealing with some problems when resolving the problem is not viable or cost-effective. In this case, the problem remains in the known error status, and the documented workaround is applied should related incidents occur. Every documented workaround should include a clear definition of the symptoms to which it applies. In some cases, workaround application can be automated.

For other problems, a way to fix the error should be found. This is a part of error control. Error control activities manage known errors, which are problems where initial analysis has been completed; it usually means that faulty components have been identified. Error control also includes identification of potential permanent solutions which may result in a change request for implementation of a solution, but only if this can be justified in terms of cost, risks, and benefits.

Error control regularly re-assesses the status of known errors that have not been resolved, including overall impact on customers, availability and cost of permanent resolutions, and effectiveness of workarounds. The effectiveness of workarounds should be evaluated each time a workaround is used, as the workaround may be improved based on the assessment.

Problem management activities are very closely related to incident management. The practices need to be designed to work together within the value chain. Activities from these two practices may complement each other (for example, identifying the causes of an incident is a problem management activity that may lead to incident resolution), but they may also conflict (for example, investigating the cause of an incident may delay actions needed to restore service).

Examples of interfaces between problem management, risk management, change control, knowledge management, and continual improvement are as follows:

- Problem management activities can be organized as a specific case of risk management: they aim to identify, assess, and control risks in any of the four dimensions of service management. It is useful to adopt risk management tools and techniques for problem management.
- Implementation of problem resolution is often outside the scope of problem management. Problem management typically initiates resolution via change control and participates in the post-implementation review; however, approving and implementing changes is out of scope for the problem management practice.
- Output from the problem management practice includes information and documentation concerning workarounds and known errors. In addition, problem management may utilize information in a knowledge management system to

investigate, diagnose, and resolve problems.

- Problem management activities can identify improvement opportunities in all four dimensions of service management. Solutions can in some cases be treated as improvement opportunities, so they are included in a continual improvement register (CIR), and continual improvement techniques are used to prioritize and manage them, sometimes as part of a product backlog.

Many problem management activities rely on the knowledge and experience of staff, rather than on following detailed procedures. People responsible for diagnosing problems often need the ability to understand complex systems, and to think about how different failures might have occurred. Developing this combination of analytical and creative ability requires mentoring and time, as well as suitable training.

The ITIL story: Axle's problem management

Henri: *Axle participates in feedback programmes with all our car manufacturers. We share maintenance and repair data with them to help them to continually improve their services. In return, they alert us to any potential problems in our vehicles.*

Radhika: *Recently, we were alerted to a potential problem in our fleet. A car manufacturer had recalled a popular model in our fleet to fix an error found in the airbag activation system.*

Su: *Fortunately it was found before Axle experienced any incidents, but there was still the potential for issues to occur, which meant it was a problem we had to deal with.*

Marco: *We follow a similar practice for our other systems and services, including all of the IT components we use.*

Radhika: *Axle's incident management practice is one of our most important sources of information on errors in our systems. Any major incident we experience is followed by an investigation into the possible causes. Sometimes this will lead us to find and fix errors in the systems, and we often identify ways to decrease the number of incidents Axle will have in the future.*

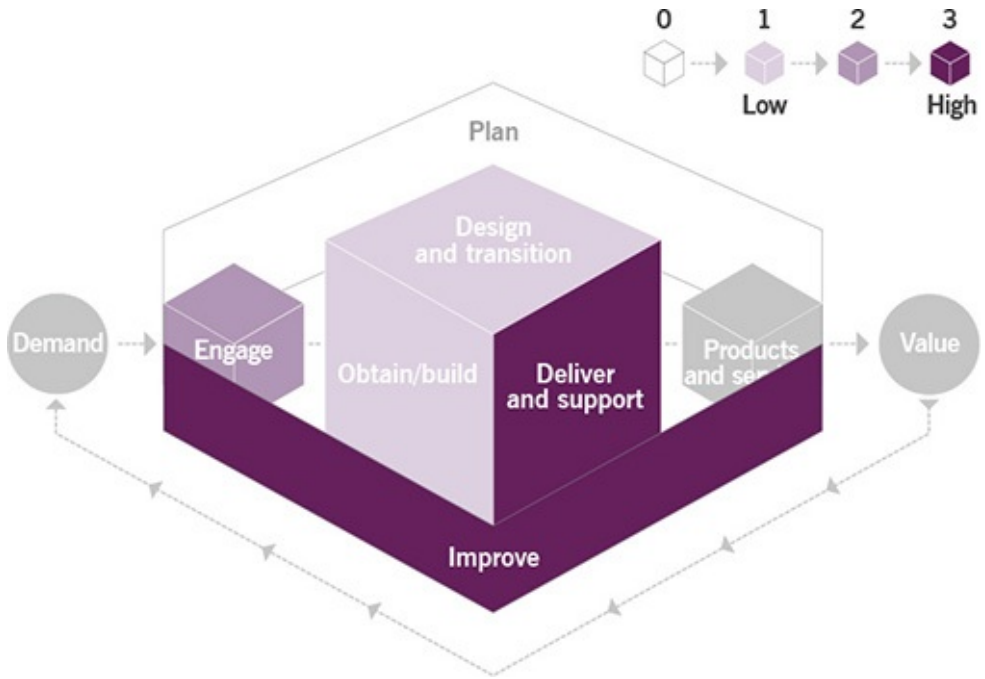

Figure 5.24 Heat map of the contribution of problem management to value chain activities

Problem management is usually focused on errors in operational environments. Figure 5.24 shows the contribution of problem management to the service value chain, with the practice being applied mainly to the improve, and deliver and support value chain activities:

- Improve This is the main focus area for problem management. Effective problem management provides the understanding needed to reduce the number of incidents and the impact of incidents that can't be prevented.
- Engage Problems that have a significant impact on services will be visible to customers and users. In some cases, customers may wish to be involved in problem prioritization, and the status and plans for managing problems should be communicated. Workarounds are often presented to users via a service portal.
- Design and transition Problem management provides information that helps to improve testing and knowledge transfer.
- Obtain/build Product defects may be identified by problem management; these are then managed as part of this value chain activity.
- Deliver and support Problem management makes a significant contribution by preventing incident repetition and supporting timely incident resolution.

5.2.9 Release management

Key message

The purpose of the release management practice is to make new and changed services and features available for use.

Definition: Release

A version of a service or other configuration item, or a collection of configuration items, that is made available for use.

A release may comprise many different infrastructure and application components that work together to deliver new or changed functionality. It may also include documentation, training (for users or IT staff), updated processes or tools, and any other components that are required. Each component of a release may be developed by the service provider or procured from a third party and integrated by the service provider.

Releases can range in size from the very small, involving just one minor changed feature, to the very large, involving many components that deliver a completely new service. In either case, a release plan will specify the exact combination of new and changed components to be made available, and the timing for their release.

A release schedule is used to document the timing for releases. This schedule should be negotiated and agreed with customers and other stakeholders. A release post-implementation review enables learning and improvement, and helps to ensure that customers are satisfied.

In some environments, almost all of the release management work takes place before deployment, with plans in place as to exactly which components will be deployed in a particular release. The deployment then makes the new functionality available.

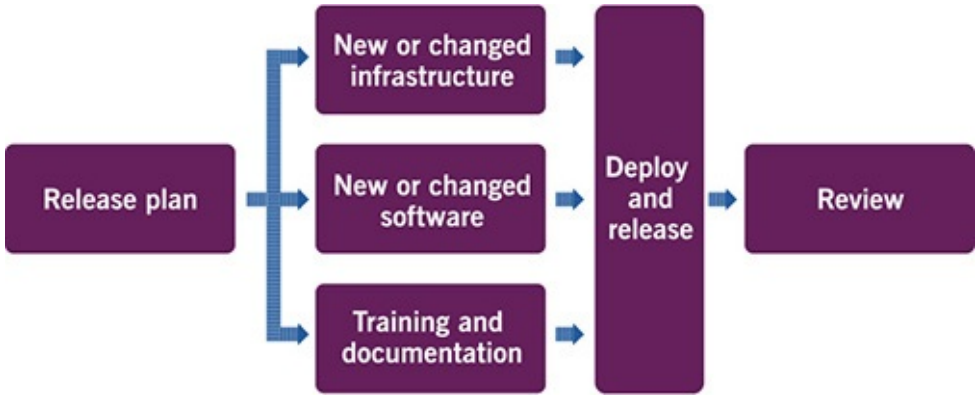

Figure 5.25 Release management in a traditional/waterfall environment

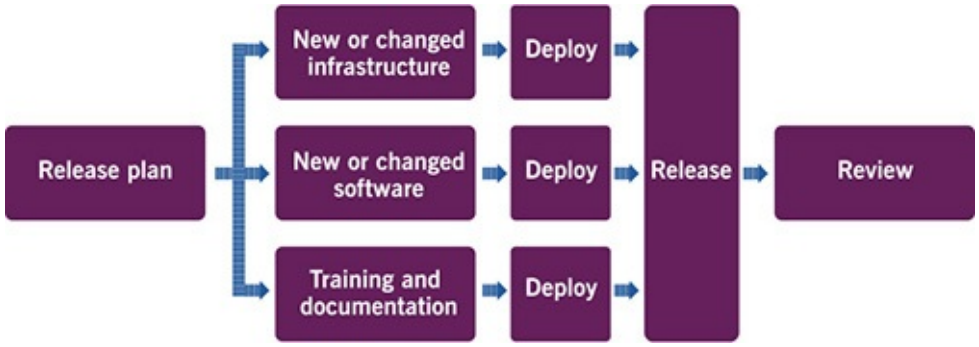

Figure 5.26 Release management in an Agile/DevOps environment

Figure 5.25 shows how release management is handled in a traditional/waterfall environment. In these environments release management and deployment may be combined and executed as a single process.

In an Agile/DevOps environment there can be significant release management activity after deployment. In these cases, software and infrastructure are typically deployed in many small increments, and release management activity enables the new functionality at a later point. This may be done as a very small change. Figure 5.26 shows how release management is handled in such an environment.

Release management is often staged, with pilot releases being made available to a small number of users to ensure that everything is working correctly before the release is given to additional groups. This staged approach can work with either of the two sequences shown in Figures 5.25 and 5.26. Sometimes a release must be made available to all users at the same time, as when a major restructuring of the underlying shared data is required.

Staging of a release is often achieved using blue/green releases or feature flags:

- Blue/green releases use two mirrored production environments. Users can be switched to an environment that has been updated with the new functionality by use of network tools that connect them to the correct environment.

- Feature flags enable specific features to be released to individual users or groups in a controlled way. The new functionality is deployed to the production environment without being released. A user configuration setting then releases the new functionality to individual users (or groups of users) as needed.

In a DevOps environment, release management is often integrated with the continuous integration and continuous delivery toolchain. The tools of release management may be the responsibility of a dedicated person, but decisions about the release can be made by the development team. In a more traditional environment, releases are enabled by the deployment of the components. Each release is described by a release record on an ITSM tool. Release records are linked to CIs and change records to maintain information about the release.

Components of a release are often provided by third parties. Examples of third-party components include cloud infrastructure, software as a service components, and third-party support. It is also common to include third-party software, or open-source software, as part of application development. Release management needs to work across organizational boundaries to ensure that all components are compatible and to provide a seamless experience for users. It also needs to consider the impact of changes to third-party components, and to plan for how these will be released.

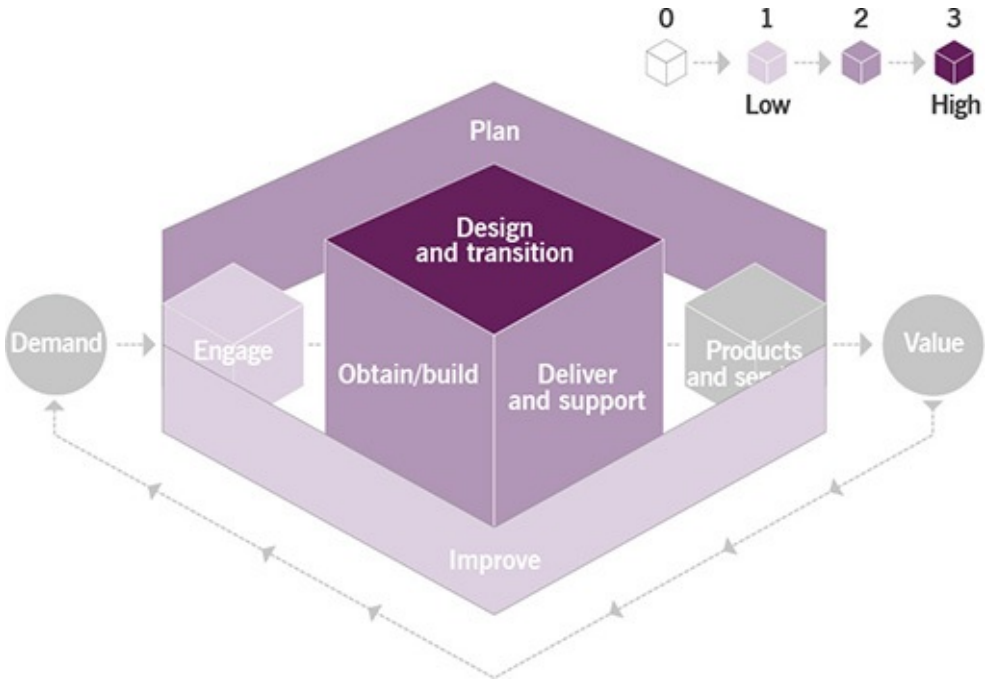

Figure 5.27 Heat map of the contribution of release management to value chain activities

Figure 5.27 shows the contribution of release management to the service value chain, with the practice being involved in all value chain activities:

- Plan Policies, guidance, and timelines for releases are driven by the organizational strategy and service portfolio. The size, scope, and content of each release should be planned and managed.
- Improve New or changed releases may be required to deliver improvements, and these should be planned and managed in the same way as any other release.
- Engage The content and cadence of releases must be designed to match the needs and expectations of customers and users.
- Design and transition Release management ensures that new or changed services are made available to customers in a controlled way.
- Obtain/build Changes to components are normally included in a release, delivered in a controlled way.
- Deliver and support Releases may impact on delivery and support. Training, documentation, release notes, known errors, user guides, support scripts, etc. are provided by this practice to facilitate service restoration.

The ITIL story: Axle's release management

Marco: *When we release updates to our booking app, we make sure they're accompanied by user awareness and marketing campaigns for our users, customers, and teams. We provide specific training for the service desk and support teams that are internal and external.*

Radhika: *Some changes may need extra support or the introduction of new components. For example, Axle Aware was released with a new user manual to explain the system. We also made sure the Aware system could sync with the Axle booking app before we released it.*

Henri: *The support given to the new app and Axle Aware has really helped the release of both of these new offerings, leading to great first impressions and a strong level of adoption amongst our users and customers, as well as our own teams.*

5.2.10 Service catalogue management

Key message

The purpose of the service catalogue management practice is to provide a

single source of consistent information on all services and service offerings, and to ensure that it is available to the relevant audience.

The list of services within the service catalogue represents those which are currently available and is a subset of the total list of services tracked in the service provider's service portfolio. Service catalogue management ensures that service and product descriptions are expressed clearly for the target audience to support stakeholder engagement and service delivery. The service catalogue may take many forms such as a document, online portal, or a tool that enables the current list of services to be communicated to the audience.

5.2.10.1 Service catalogue management activities

The service catalogue management practice includes an ongoing set of activities related to publishing, editing, and maintaining service and product descriptions and their related offerings. It provides a view on the scope of what services are available, and on what terms. The service catalogue management practice is supported by roles such as the service owner and others responsible for managing, editing, and keeping up to date the list of available services as they are introduced, changed, or retired.

Tailored views

As described above, the service catalogue enables the creation of value and is used by many different practices within the service value chain. Because of this, it needs to be flexible regarding what service details and attributes it presents, based on its intended purpose. As such, organizations may wish to consider providing different views of the catalogue for different audiences.

The full list of services within a service catalogue may not be applicable to all customers and/or users. Likewise, the various attributes of services such as technical specifications, offerings, agreements, and costs are not applicable to all service consumer types. This means that the service catalogue should be able to provide different views and levels of detail to different stakeholders. Examples of views include:

- User views Provide information on service offerings that can be requested, and on provisioning details.
- Customer views Provide service level, financial, and service performance data.
- IT to IT customer views Provide technical, security, and process information for use in service delivery.

While multiple views of the service catalogue are possible, the creation of separate or isolated service catalogues within different technology systems should be avoided if possible as this will promote segregation, variability, and complexity.

For the service catalogue to be perceived as useful by the customer organization it must do more than provide a static platform for publishing information about IT services. Unless the service catalogue enables customer engagement by supporting discussions related to standard and non-standard service offerings and/or automates request and order fulfilment processes, the chances of its ongoing adoption as a useful and meaningful resource are minimal. For this reason, the views of many organizations on the service catalogue are focused on the consumable or orderable elements of service offerings. These are often called request catalogues.

Definition: Request catalogue

A view of the service catalogue, providing details on service requests for existing and new services, which is made available for the user.

Figure 5.28 shows the contribution of service catalogue management to the service value chain, with the practice being involved in all value chain activities:

- Plan The service catalogue enables strategy and service portfolio investment decisions by providing details on current service scope and offerings.
- Improve Service catalogue descriptions and demand patterns are constantly monitored and evaluated to support continual improvement, alignment, and value creation.
- Engage The service catalogue enables strategic, tactical, and operational relationships with customers and users by enabling and potentially automating various aspects of practices such as relationship management, request management, and the service desk.

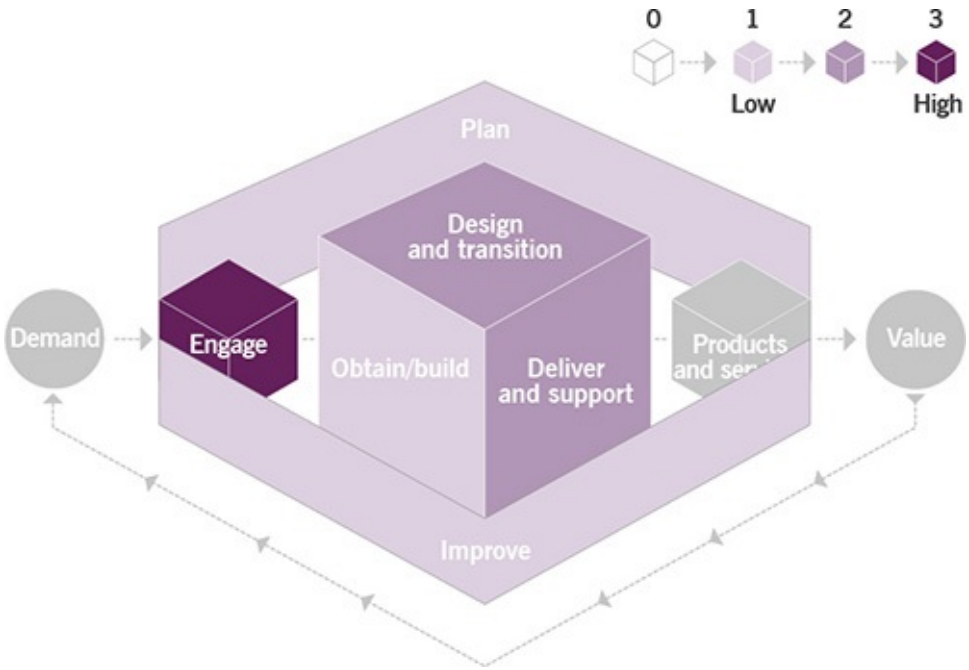

Figure 5.28 Heat map of the contribution of service catalogue management to value chain activities

- Design and transition The service catalogue ensures both the utility and warranty aspects of services are considered and published, including the information security policy, IT service continuity levels, service level agreements, and service offerings. Additional activities include the definition and creation of service descriptions, request models, and views to be published.
- Obtain/build Service catalogue management supports this value chain activity by providing service catalogue views for procurement of components and services.
- Deliver and support The service catalogue provides context for how the service will be delivered and supported, and publishes expectations related to agreements and performance.

5.2.11 Service configuration management

Key message

The purpose of the service configuration management practice is to ensure that accurate and reliable information about the configuration of services, and the CIs that support them, is available when and where it is needed. This includes information on how CIs are configured and the relationships between

them.

Definition: Configuration item

Any component that needs to be managed in order to deliver an IT service.

Service configuration management collects and manages information about a wide variety of CIs, typically including hardware, software, networks, buildings, people, suppliers, and documentation. Services are also treated as CIs, and configuration management helps the organization to understand how the many CIs that contribute to each service work together. Figure 5.29 is a simplified diagram showing how multiple CIs contribute to an IT service.

Configuration management provides information on the CIs that contribute to each service and their relationships: how they interact, relate, and depend on each other to create value for customers and users. This includes information about dependencies between services. This high-level view is often called a service map or service model, and forms part of the service architecture.

It is important that the effort needed to collect and maintain configuration information is balanced with the value that the information creates. Maintaining large amounts of detailed information about every component, and its relationships to other components, can be costly, and may deliver very little value. The requirements for configuration management must be based on an understanding of the organization's goals, and how configuration management contributes to value creation.

The value created by configuration management is indirect, but enables many other practices to work efficiently and effectively. As such, planning for configuration management should start by understanding who needs the configuration information, how it will be used, what is the best way for them to obtain it, and who can maintain and update this information. Sometimes it can be more efficient to simply collect the information when it is needed, rather than to have it collected in advance and maintained, but on other occasions it is essential to have information available in a configuration management system (CMS). The type and amount of information recorded for each type of CI should be based on the value of that information, the cost of maintaining it, and how the information will be used.

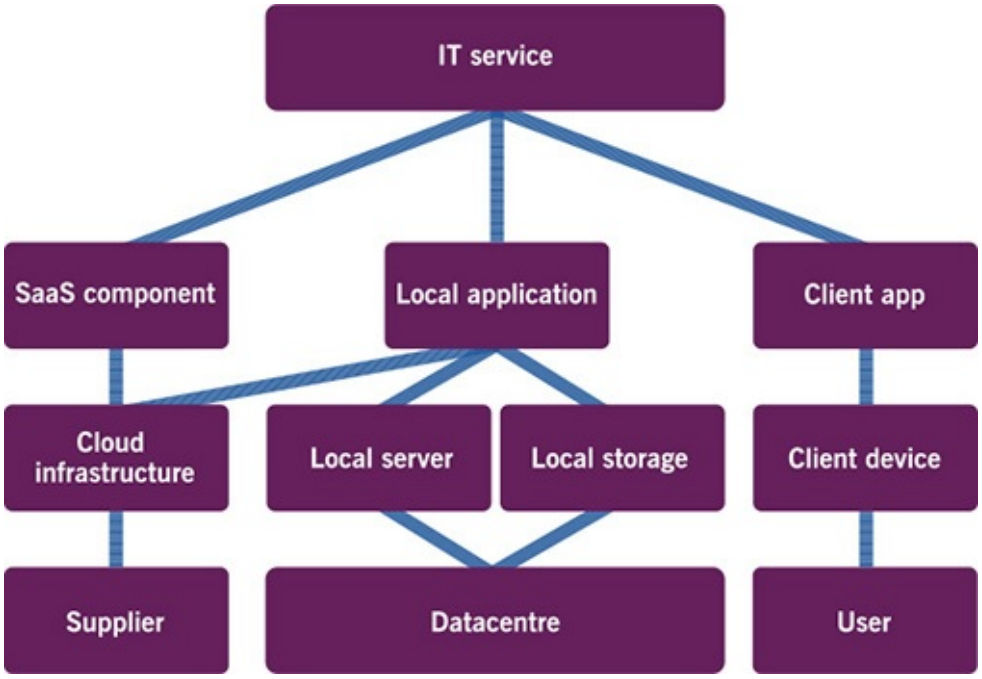

Figure 5.29 Simplified service model for a typical IT service

Definition: Configuration management system

A set of tools, data, and information that is used to support service configuration management.

Configuration information should be shared in a controlled way. Some information could be sensitive; for example, it could be useful to someone trying to breach security controls, or it could include personal information about users, such as phone numbers and home addresses.

Configuration information can be stored and published in a single configuration management database (CMDB) for the whole organization, but it is more common for it to be distributed across several sources. In either case it is important to maintain links between configuration records, so that people can see the full set of information they need, and how the various CIs work together. Some organizations federate CMDBs to provide an integrated view. Others may maintain different types of data; for example, having separate data stores for asset management data (see section 5.2.6), configuration details, service catalogue information, and high-level service models.

Tools that are used to log incidents, problems, and changes need access to

configuration records. For example, an organization trying to identify problems with a service may need to find incidents related to a specific software version, or model of disk drive. The understanding of the need for this information helps to establish what CI attributes should be stored for this organization; in this case software versions and disk drive models. To diagnose incidents, visibility of recent changes to the affected CIs may be needed, so relationships between CIs and changes must be maintained.

Many organizations use data collection tools to gather detailed configuration information from infrastructure and applications, and use this to populate a CMS. This can be effective, but can also encourage the collection of too much data without sufficient information on relationships, and how the components work together to create a service. Sometimes configuration information is used to actually create the CI, rather than just to document it. This approach is used for 'infrastructure as a code', where information on the infrastructure is managed in a data repository and used to automatically configure the environment.

A large organization may have a team that is dedicated to configuration management. In other organizations this practice can be combined with change control, or there can be a team responsible for change, configuration, and release management. Some organizations apply a distributed model where functional teams take ownership of updating and maintaining the CIs within their control and oversight.

Configuration management typically needs processes to:

- identify new CIs, and add them to the CMS
- update configuration data when changes are deployed
- verify that configuration records are correct
- audit applications and infrastructure to identify any that are not documented.

Figure 5.30 shows the contribution of configuration management to the service value chain, with the practice being involved in all value chain activities:

- Plan Configuration management is used for planning new or changed services.
- Improve Configuration management, like every other aspect of service management, should be subject to measurement and continual improvement. Since the value of configuration management typically comes from how it facilitates other practices, it is important to understand what use these practices are making of configuration information, and then identify how this can be improved.
- Engage Some stakeholders (partners and suppliers, consumers, regulators, etc.) may require and use configuration information, or provide their configuration information to the organization.
- Design and transition Configuration management documents how assets work

together to create a service. This information is used to support many value chain activities, and is updated as part of the transition activity.

- Obtain/build Configuration records may be created during this value chain activity, describing new or changed services and components. Sometimes configuration records are used to create the code or artefact that is being built.
- Deliver and support Information on CIs is essential to support service restoration. Configuration information is used to support activities of the incident management and problem management practices.

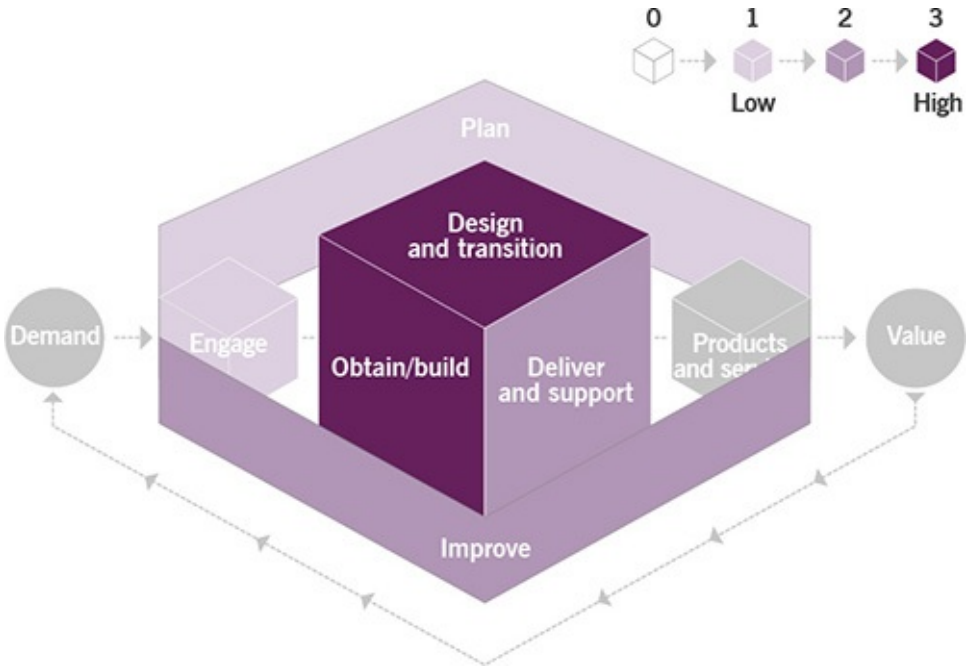

Figure 5.30 Heat map of the contribution of service configuration management to value chain activities

5.2.12 Service continuity management

Key message

The purpose of the service continuity management practice is to ensure that the availability and performance of a service are maintained at sufficient levels in case of a disaster. The practice provides a framework for building organizational resilience with the capability of producing an effective response that safeguards the interests of key stakeholders and the organization's reputation, brand, and value-creating activities.

Service continuity management supports an overall business continuity management (BCM) and planning capability by ensuring that IT and services can be resumed within required and agreed business timescales following a disaster or crisis. It is triggered when a service disruption or organizational risk occurs on a scale that is greater than the organization's ability to handle it with normal response and recovery practices such as incident and major incident management. An organizational event of this magnitude is typically referred to as a disaster.

Each organization needs to understand what constitutes a disaster in its own context. Establishing what is meant by a disaster must be considered and defined prior to a trigger event at both an organizational and on a per-service level using a business impact analysis. The Business Continuity Institute defines a disaster as:

> '…a sudden unplanned event that causes great damage or serious loss to an organization. It results in an organization failing to provide critical business functions for some predetermined minimum period of time.'

The sources that trigger a disaster response and recovery are varied and complex, as are the number of stakeholders and the different aspects of potential organizational impact. The complex risk management conditions related to the examples in Table 5.3 make it imperative that the service continuity management practice be thoroughly thought out, designed for flexibility, and tested on a regular basis to ensure that services can be recovered at a speed necessary for business survival.

Table 5.3 Examples of disaster sources, stakeholders involved, and organizational impact

Disaster sources	Stakeholders involved	Organizational impact
Supply chain failure	Employees	Lost income
Terrorism	Executives	Damaged reputation
Weather	Governing body	Loss of competitive advantage
Cyber attack	Suppliers	Breach of law, health and safety regulations
Health emergency	IT teams	
Political or economic event	Customers	Risk to personal safety
Technology failure	Users	Immediate and long-term loss of market share
Public crisis	Communities	

Definitions

- Recovery time objective (RTO) The maximum acceptable period of time following a service disruption that can elapse before the lack of business functionality severely impacts the organization. This represents the

maximum agreed time within which a product or an activity must be resumed, or resources must be recovered.

- Recovery point objective (RPO) The point to which information used by an activity must be restored to enable the activity to operate on resumption.
- Disaster recovery plans A set of clearly defined plans related to how an organization will recover from a disaster as well as return to a pre-disaster condition, considering the four dimensions of service management.
- Business impact analysis (BIA) A key activity in the practice of service continuity management that identifies vital business functions (VBFs) and their dependencies. These dependencies may include suppliers, people, other business processes, and IT services. BIA defines the recovery requirements for IT services. These requirements include RTOs, RPOs, and minimum target service levels for each IT service.

Service continuity management versus incident management

Service continuity management focuses on those events that the business considers significant enough to be treated as a disaster. Less significant events will be dealt with as part of incident management or major incident management. The distinction between disasters, major incidents, and incidents needs to be pre-defined, agreed, and documented with clear thresholds and triggers for calling the next tier of response and recovery into action without unnecessary delay and risk.

As organizations have become increasingly dependent on technology-enabled services, the need for high-availability solutions has become critical to organizational resilience and competitiveness. Organizations achieve high availability through a combination of business planning, technical architecture resilience, availability planning, proactive risk, and information security management, as well as through incident management and problem management.

Figure 5.31 shows the contribution of service continuity management to the service value chain, with the practice being involved in all value chain activities:

- Plan The organization's leadership and governing body establish an initial risk appetite for the organization with defined scope, policies, supplier strategies, and investment in recovery options. Service continuity management supports this with relevant information about the current continuity status of the organization and with tools and methods for planning and forecasting.
- Improve Service continuity management ensures that continuity plans, measures, and mechanisms are continually monitored and improved in line with changing internal and external circumstances.

- Engage Engagement with various stakeholders to provide assurance with regard to an organization's readiness for disasters is supported by this practice.
- Design and transition Service continuity management ensures that products and services are designed and tested according to the organization's continuity requirements.

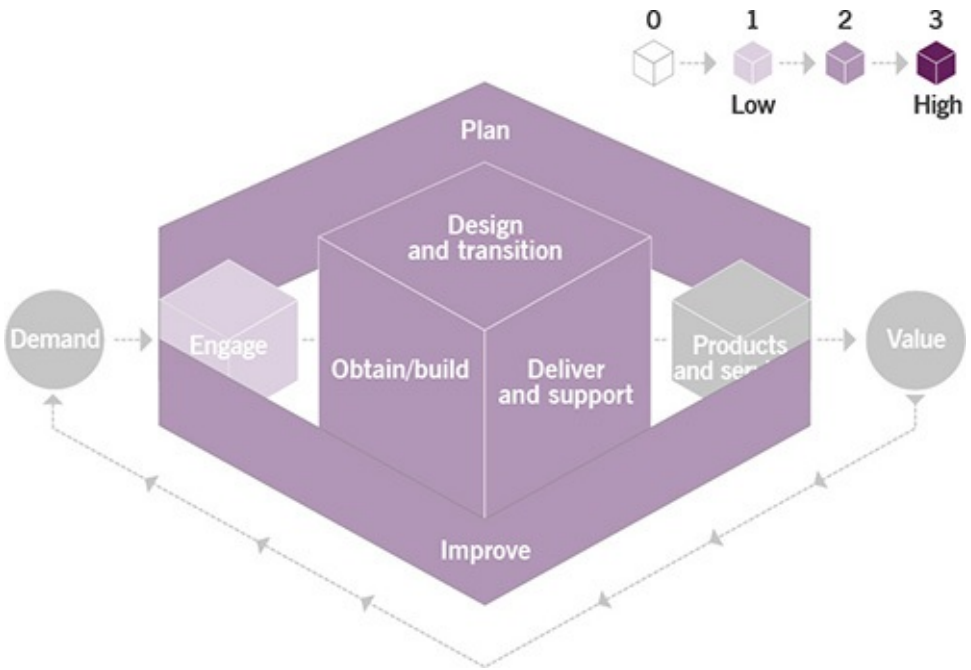

Figure 5.31 Heat map of the contribution of service continuity management to value chain activities

- Obtain/build Service continuity management ensures that continuity is built into the organization's services and components, and that procured components and services meet the organization's continuity requirements.
- Deliver and support Ongoing delivery, operations, and support are performed in accordance with continuity requirements and policies.

5.2.13 Service design

Key message

The purpose of the service design practice is to design products and services that are fit for purpose, fit for use, and that can be delivered by the organization and its ecosystem. This includes planning and organizing people,